WE CLAIM

1. A method, comprising:

analyzing a transport stream; and

preparing the transport stream for processing that bypasses encrypted portions of the transport stream.

2. A method according to Claim 1, wherein analyzing the transport stream includes determining which portions of the transport stream are to pass unencrypted.

3. A method according to Claim 2, wherein determining which portions of the transport stream are to pass unencrypted is executed based on a statistical analysis.

4. A method according to Claim 2, wherein determining which portions of the transport stream are to pass unencrypted is executed dynamically.

5. A method according to Claim 2, wherein determining which portions of the transport stream are to pass unencrypted includes determining a permissible incursion beyond a packet header to gather data for the processing.

6. A method according to Claim 2, wherein determining which portions of the transport stream are to pass unencrypted includes detecting a data packet containing at least a portion of a packetized elementary stream (PES) header.

7. A method according to Claim 2, wherein determining which portions of the transport stream are to pass unencrypted includes detecting bytes of data that are required for processing the transport stream.

8. A method according to Claim 1, wherein preparing the transport stream for processing includes encrypting portions of the transport stream that are not to pass unencrypted.

9. A method according to Claim 1, wherein preparing the transport stream for processing includes encrypting packets containing PES payload data.

10. A method according to Claim 1, wherein preparing the transport stream for processing includes leaving a packet containing a portion of a frame header unencrypted.

11. A method according to Claim 1, wherein preparing the transport stream for processing includes leaving bytes of data unencrypted that are required for processing the transport stream.

12. A method according to Claim 1, wherein preparing the transport stream for processing includes common scrambling packets composed of PES payload data.

13. A method according to Claim 1, wherein preparing the transport stream for processing includes:

generating a multiplex-compliant encryption method packet; and

inserting the multiplex-compliant encryption method packet into the transport stream.

14. A method according to Claim 13, wherein the encryption method packet identifies an encryption algorithm used in preparing the transport stream for processing, identifies encrypted portions of the transport stream, and provides data for deriving a decryption key.

15. A method according to Claim 13, wherein the encryption method packet identifies an unencrypted portion of the transport stream, a location of the encrypted portion of the unencrypted portion of the transport stream, and a process corresponding to the unencrypted portion of the transport stream.

16. A method according to Claim 13, wherein the encryption method packet is delivered via a private table.

17. A method, comprising:

receiving a partially encrypted transport stream; and

processing the transport stream in a manner that bypasses encrypted portions of the transport stream.

18. A method according to Claim 17, further comprising:

receiving a multiplex-compliant encryption method packet corresponding to the transport stream; and

decrypting encrypted portions of the transport stream using a decryption key.

19. A method according to Claim 18, wherein the decryption key is included in the encryption method packet or is received in an out-of-band message.

20. A method according to Claim 17, wherein processing the transport stream includes demultiplexing the transport stream based on unencrypted portions of the transport stream.

21. A method according to Claim 17, wherein processing the transport stream includes indexing payload data contained in the transport stream based on unencrypted portions of the transport stream.

22. A computer-readable medium having one or more instructions that are executable by one or more processors, the one or more instructions causing the one or more processors to:

determine which portions of a transport stream are to pass unencrypted for processing that disregards encrypted portions of the transport stream; and

prepare the transport stream for the processing.

23. A computer-readable medium according to Claim 22, wherein the one or more instructions to determine which portions of the transport stream are to pass unencrypted cause the one or more processors to leave unencrypted data packets having at least a portion of a PES header.

24. A computer-readable medium according to Claim 22, wherein the one or more instructions to determine which portion of the transport stream are to pass unencrypted cause the one or more processors to leave unencrypted bytes of data required for processing the transport stream.

25. A computer-readable medium according to Claim 22, wherein the one or more instructions to determine which portions of the transport stream are to pass unencrypted cause the one or more processors to leave unencrypted a threshold amount of data beyond packet header data that is relevant for the processing.

26. A computer-readable medium according to Claim 22, wherein the one or more instructions to prepare the transport stream for the processing cause the one or more processors to encrypt portions of the transport stream that are not to pass unencrypted.

27. A computer-readable medium according to Claim 26, wherein the one or more instructions causing the one or more processors to encrypt portions of the transport stream applies an advanced encryption standard (AES)-counter (CTR) mode cipher.

28. A computer-readable medium according to Claim 26, comprising one or more further instructions causing the one or more processors to:

generate a multiplex-compliant encryption method packet; and

insert the multiplex-compliant encryption method packet into the transport stream.

29. A computer-readable medium according to Claim 22, wherein the encryption method packet identifies an encryption algorithm used to prepare the transport stream for processing, identifies encrypted portions of the transport stream, and provides at least a basis for key to decrypt the encrypted portions of the transport stream.

30. A computer-readable medium according to Claim 22, wherein the encryption method packet identifies an unencrypted portion of the transport stream, a location of the unencrypted portion of the transport stream, and a process associated with the unencrypted portion of the transport stream.

31. A computer-readable medium having one or more instructions that are executable by one or more processors, the one or more instructions causing the one or more processors to:

receive a partially encrypted transport stream; and

process the transport stream based on unencrypted portions of the transport stream.

32. A computer-readable medium according to Claim 31, comprising one or more further instructions causing the one or more processors to:

receive a multiplex-compliant encryption method packet corresponding to the transport stream; and

decrypt encrypted portions of the transport stream using an encryption key based in the encryption method packet.

33. A computer-readable medium according to Claim 31, wherein the one or more instructions to process the transport stream cause the one or more processors to demultiplex the transport stream based on unencrypted portions of the transport stream.

34. A computer-readable medium according to Claim 31, wherein the one or more instructions to process the transport stream cause the one or more processors to index payload data contained in the transport stream based on unencrypted portions of the transport stream.

35. An apparatus, comprising:

an analyzer to determine which portions of a transport stream are to pass unencrypted for processing that does not incorporate encrypted portions of the transport stream; and

a scrambler to encrypt other portions of the transport stream based on the determination.

36. An apparatus according to Claim 35, wherein the analyzer is to dynamically determine that a threshold incursion into payload data is to pass unencrypted in order to process the transport stream without removing the encryption from other portions of the transport stream.

37. An apparatus according to Claim 35, wherein the analyzer is to determine that a packet containing at least a portion of a PES header is to pass unencrypted.

38. An apparatus according to Claim 35, wherein the analyzer is to determine that data arbitrarily disposed throughout PES payload data are to pass unencrypted.

39. An apparatus, comprising:

means for determining which portions of a transport stream are to pass unencrypted for processing that does not incorporate encrypted portions of the transport stream; and

means for encrypting other portions of the transport stream in accordance with the analysis.

40. An apparatus according to Claim 39, wherein the means for determining designates a dynamically determined amount of payload data to pass unencrypted in order to process the transport stream without removing the encryption from other portions of the transport stream.